Internet Security Management – a Challenging Joint Postgraduate Curriculum Design

Helen Armstrong
School of Information Systems
Curtin University of Technology
GPO Box U1987
Perth, Western Australia 6845
Australia
Email: H.Armstrong@curtin.edu.au
Phone: +61-8-9266 7017

Abstract
This paper describes the design of a joint program in Internet Security Management between the Schools of Information Systems and Computer Science. An overview of the curriculum is given, and the roles played by each School in the teaching of the courses described. The advantages and hurdles of designing offerings across independent Schools is also discussed.

Keywords: Internet Security, Internet Security Management, Curriculum Design, Postgraduate Studies

Introduction

With the growth in cybercrime comes a realisation that organisations need to address the security of their information and associated information systems networks. The call for more educational programs in information security has emerged from both the private and public sectors, government agencies promoting specialist education and business organisations with a professional need for information security expertise.

A media release in February 2001 by Senator the Hon Richard Alston, Minister for Communications, Information Technology and the Arts (NOIE, 2001a), states that Information Security is a major national priority in Australia. In addition, the draft Report on E-Security R&D in Australia released by the National Office for the Information Economy states that "The [Australian] Government has a clear role to protect information infrastructure, which is critical to national security, and protect the public from criminal or malicious activity occurring through electronic mediums, primarily the Internet." (NOIE, 2001b).

In response to these national priorities and the needs of industry and government, Curtin University has designed a postgraduate program in Internet Security Management. The program is run jointly by the School of Computing and the School of Information Systems, and attempts to balance the technical, conceptual and human skills required to meet the above challenge.

In order to meet these growing demands, two Schools within Curtin University of Technology in Perth, Western Australia, joined forces to offer postgraduate studies specialising in Internet Security Management. The curriculum aims to produce graduates with generic, technical and management skills in the field of Internet security.

The aim of this paper is to discuss the design of the postgraduate curriculum in Internet security management across two academic schools in differing faculties within a university. The advantages of a joint program are discussed along with the problems encountered in the design process.

Overview of the Internet Security Management Programs

The new programs are designed for students who have completed a Bachelor degree in a computing related discipline. Students embarking on the programs require an understanding of computer programming, operating systems, networks and computer architecture.

The new program is offered at three levels-

- Postgraduate Diploma in Internet Security Management
- Master of Internet Security Management - professional masters degree
- Master of Commerce (Internet Security Management) – masters degree by coursework

The structure of the programs is illustrated in Table 1.

Postgraduate Diploma in Internet Security Management

This program is designed for students who wish to enhance skills and knowledge in the design and management of Internet security and electronic commerce in business organisations. The program comprises eight units of study each carrying 25 credit points, totalling 200 credit points. The postgraduate diploma course can be completed in one year (two semesters) of full-time study or two years of part-time study.

The program comprises eight units of study covering information security management, problem-solving, computer networks and communications, organisational behaviour, JAVA programming, research methods, project management, distributed computing and database design and security.

The postgraduate diploma articulates to either the Master of Internet Security Management or the Master of Commerce (Internet Security Management).

Master of Internet Security Management

This course is a professional masters degree containing a total of twelve units of study. It is designed for computing professionals who wish to take leadership roles in the management of Internet security. Students need a computing-related degree plus a minimum of two-years relevant industry experience to enter this program. This course can be completed in eighteen months (three semesters) of full-time study or three years of part-time study.

The first eight units of the Master of Internet Security Management are the same as the Postgraduate Diploma course, with four additional units required to complete the degree. Computer forensics is a core unit of study in the masters program, and students may choose three optional units or undertake a research project. Optional study units include software security and encryption, business intelligence and cyberwarfare, web site management, electronic commerce security, XML programming, JAVA programming, Internet law, networking and mobile communications, machine perception and artificial intelligence.

There is no direct articulation from this professional masters to other masters degrees or doctorates. Students wishing to progress to doctoral studies are advised to enrol in the masters by coursework, or a masters by research in preference to this program.

Study Plan Full-time	Postgraduate Diploma in Internet Security Management	Master of Internet Security Management	Master of Commerce (Internet Security Management)
Year 1 Sem 1	Network & Communications Security Information Security Management Problem Solving Organisational Behaviour Or JAVA Programming	Network & Communications Security Information Security Management Problem Solving Organisational Behaviour Or JAVA Programming	Network & Communications Security Information Security Management Problem Solving Organisational Behaviour Or JAVA Programming
Year 1 Sem 2	Project & Risk Management Database Design & Security Distributed Computing & CORBA Research Methods	Project & Risk Management Database Design & Security Distributed Computing & CORBA Research Methods	Project & Risk Management Database Design & Security Distributed Computing & CORBA Research Methods
Year 2 Sem 1		Computer Forensics 1 Optional Unit Plus Either: Security Project (50 credits = 2 units) or 2 Optional Units	Computer Forensics 3 Optional Units
Year 2 Sem 2			Security Project & Dissertation (100 credits = 4 units)
Sem = Semester		**Optional Units:** Networking & Mobile Communications Advanced JAVA Programming XML Programming Business Intelligence & Cyberwarfare E Commerce Security Web Site Management Internet Law Machine Perception Artificial & Machine Intelligence	

Table 1: Structure of the Internet Security Management Programs

Master of Commerce (Internet Security Management)
This course is designed for students who wish to continue their studies in Internet security management to gain further knowledge and skills in managing Internet security and electronic commerce environments. Unlike the professional masters degree students do not need relevant industry experience to undertake this course. The total program is 200 credit points containing a mix of eight coursework and research units. The Master of Commerce (ISM) consists of two stages, the first stage is the Postgraduate Diploma in ISM, the second stage is the Masters component. The Masters component has a duration of one year (two semesters) of full-time study or two years of part-time study.

The first eight units of study in stage one are the same as the Postgraduate Diploma in ISM above. The Masters stage comprises a unit of study on computer forensics and a choose of three other units of study from software security and encryption, business intelligence and cyberwarfare, web site management, electronic commerce security, XML programming, JAVA programming, Internet law, networking and mobile communications, machine perception and artificial intelligence.

The final component is a substantial research project in a security related area, resulting in a dissertation. The size of the research project must be equivalent to four units, or one full-time semester of study. This project is written up as a research dissertation, assessed by two examiners, and published by the university, thus satisfying the entrance requirements for doctoral studies.

Collaboration on the Joint Program Design

There are many advantages and challenges in a joint program of this nature. This project has required the commitment of both schools to the time and resources required to design, develop and run these programs. The content has been based upon a shared understanding that an Internet Security Management professional needs to be holistic in approach, requiring generic, technical and practical skills. In addition, the joint offerings have provided students the opportunity to gain a much broader set of skills and knowledge. Computer Science students are exposed to computing in a business and organisational context, while Information Systems students acquire a greater depth of technical knowledge and expertise. The need for a graduate with a more rounded skill-set is thus met.

Recognition of each other's strengths and expertise has emerged from the curriculum design process. Agreement on the technical and management content has proven to be a challenge, particularly with regard to pre-requisite knowledge for the technical areas and sequencing of the courses. Difficulties arose where students with an IT undergraduate degree were considered to have insufficient technical knowledge to undertake some of the Computer Science owned units. Some of the advanced Computer Science units required a number of pre-requisite units only offered by that School. In addition, units are usually offered in either semester 1 or semester 2, not both. This added complexity to the sequencing of units to be studied, juggling units containing pre-requisite knowledge with the semesters offered. Fortunately, the two schools currently work closely together, recognising duplications in units of study, and allowing students to undertake optional units in the other school.

Funding of staff and teaching resources within a university is a complicated matter. Sharing staff and resources across two different schools in different faculties is quite complex. The larger the body, the slower it moves, and the university is a unique organism. In order to work within the restricted University systems, the two Schools have agreed to share the teaching equally. Units offered by each school utilise resources from that school – for example, a unit owned by the School of Information Systems is taught by staff within that school using classrooms and laboratories under the control of that school. This is not the desired approach, however, as team teaching involving staff from both schools would have been the preferred teaching mode.

The new program has raised the requirement within both schools for isolated laboratories to carry out practical work and it has been necessary to hire appropriate laboratories from other schools within Curtin University for the initial running of some of the new units. New laboratories are currently being fitted to meet the requirements of the new programs. Administration of joint programs across more than one school is best handled by only one of the stakeholders. The School of Information Systems will administer the new program as the infrastructure and systems to handle the required administration are already in place within that school.

The university requires the overall program design to be approved by both Schools before being presented to the University Senate for final approval. The two schools have held numerous meetings to design the structure of the programs, define the required content, develop a logical sequence, plan semester offerings and resolve problems relating to overlapping content and prerequisite knowledge. Industry partners common to both Schools were also part of the curriculum design team.

Conclusion

The design of the new programs and their formal approval by the university has taken eighteen months. The new programs will be running in 2003 provided the university's final seal of approval is granted. The effective life of the three programs is estimated at 3-4 years, provided the unit content is regularly updated. Although the design and approval process has been time-consuming the resultant programs are promising to be in demand.

References

NOIE [2201a] Information Security – A Major Priority, Media release from the National Office for the Information Economy, Available WWW http://www.noie.gov.au/publications/media_releases/feb2001/infosecurity.htm

NOIE [2001b] Report on E-Security R&D in Australia: An Initial Assessment, National Office for the Information Economy, Canberra, Australia, June